Varnost v mobilnem telefonskem omrežju tretje generacije

Leopold Šolc

Povzetek — V mobilnem telefonskem omrežju tretje generacije so, v primerjavi z omrežjem druge generacije, uvedeni izboljšani zaščitni ukrepi. Izboljšave so posledica izkušenj iz dosedanjih omrežij in napredka tehnologije. Prispevek opisuje varnostne zahteve, razloge za izboljšave in varnostne funkcije v omrežju UMTS.

Ključne besede — Mobilna telefonska omrežja, GSM, 3G, UMTS, Varnost, VITEL 2003

Abstract — Third generation networks have improved security measures in comparison to GSM cellular networks. Better 3G-network security is result of experience gained from previous mobile network generations and improvements in technology. This paper describes security requirements, reasons for security improvements and security functions in UMTS networks.

Keywords — Cellular networks, GSM, 3G, UMTS, Security, VITEL 2003

I. UVOD

Osnovno ogrožanje varnosti mobilnih telefonskih omrežji, ki grozi tako upravljalcu omrežja kot uporabniku, je nepooblaščeno zajemanje podatkov na radijski poti in nelegalna uporaba storitev omrežja.

Z nepooblaščenim prisluškovanjem pogovoru ali z zajemanjem podatkov lahko ti izgubijo svojo zaupnost. Nadalje je s tem lahko izdana naročnikova identiteta, ki je normalno uporabljena le v okviru delovanja omrežja.

Nelegalna uporaba storitev omrežja sicer ni povezana le z nepravilnim zaračunavanjem prometa, ampak tudi s prikrivanjem identitete uporabnika. Seveda je pri vsem tem najbolj pomembno, da se stroški ustvarjenega prometa vedno pripisujejo le naročniku, ki je ta promet tudi ustvaril, saj se mu za to izda račun.

Da bi mobilna telefonska omrežja zaradi ranljivosti radijske zveze ubranili pred zlorabami, so v sodobna omrežja vpeljane ustrezne funkcije za zagotavljanje sledečih varnostnih lastnosti:

- nedvoumno prepoznavanje identitete naročnika in omrežja,
- varovanje naročnikove identitete,
- varovanje zaupnosti pogovora ali prenašanih podatkov,
- ohranjevanje tajnosti sistemskih podatkov in
- zagotavljanje pristnosti sistemskih podatkov.

Analogni sistemi, ki so v zatonu in jim razvoj tehnologije v času uvajanja ni omogočil vpeljave zanesljivih sistemskih rešitev osnovnih varnostnih zahtev, so kasneje z uvajanjem novih sistemskih funkcij v omrežja in mobilne telefone imenovane tudi mobilni terminali, dosegli visoko stopnjo varnosti. Delujoči digitalni sistemi mobilne telefonije druge generacije, kot je omrežje GSM, so imeli glede na izkušnje iz analognih omrežij zaščite rešene "celovito" že v zasnovi. Med delovanjem omrežij druge generacije se struktura varnosti ni spreminajala, čeprav so se sčasoma pokazale šibke točke v varnosti. Toda zgodile so se le manjše spremembe pri nekaterih varnostnih funkcijah. To je pravzaprav presenetljivo, saj so se delujoči digitalni sistemi snovali pred dvajsetimi leti. Če upoštevamo samo napredek računalniške tehnologije v tem času, je prav neverjetno, da se varnost v sedanjih digitalnih omrežjih ohranja še vedno na izredno visoki ravni.

II. DOBRE IN SLABE PLATI VARNOSTI V GSM OMREŽJIH

Naročnikovo identiteto v omrežju predstavlja kartica SIM. Za izpolnitev te naloge so na kartici SIM vprogramirane vse potrebne funkcije za postopek avtentikacije naročnika in so vpisani vsi potrebni sistemski podatki. Zelo važno je, da so funkcije in podatki vpisani na kartici SIM na način, ki preprečuje nepoblaščeno čitanje ali spreminjanje teh podatkov. Z uvedbo kartice SIM je ločen terminalski del mobilnega telefona od naročniškega dela. V praksi se je ta način delitve funkcij mobilnega telefona pokazal kot zelo dober, predvsem pri zmanjševanju administrativnega dela pri menjavi terminalskega dela mobilnega telefona.

Omrežje nedvoumno prepozna naročnikovo identiteto s pomočjo postopka prepoznavanja, ki je sestavljen iz dveh delov. Prvi del je prepoznavanje

naročnika, uporabnika kartice SIM, z strani kartice. Naročnik se predstavi kartici z vnosom prave kode PIN. Drugi del postopka se odvije, ko naročnik želi dostopati do storitev omrežja. Omrežje sproži avtentikacijski postopek. Postopek je zasnovan na osnovi omrežju lastnega algoritma imenovanega A3. Omrežje pošlje preko telefona v kartico SIM naključno izbrano vprašanje RAND. S pomočjo algoritma A3 in na kartici vpisanega skrivnega ključa Ki, kartica SIM izračuna odgovor SRES. SRES se preko telefona prenese v omrežje. V omrežju se izvede podoben postopek, kjer se v podsistemu omrežja imenovanem AUC izvrši podoben izračun. Ker je v podsklopu AUC shranjen enak algoritem A3 in naročniku lasten ključ Ki, mora biti tudi rezultat SRES enak. Torej, če sta vrednosti sprejetega in v AUC izračunanega odgovora SRES enaki, poskuša dostopati do storitev naročnik, ki je res naročen na storitve omrežja. Pri postopku se skriti ključ Ki nikoli ne prenaša izven varnega okolja podsklopa AUC ali iz kartice SIM. Postopek se v praksi razlikuje od opisanega. AUC ne izračunava rezultatov za vsak postopek avtentikacije, pač pa podsklop VLR poskrbi zato, da ima za vsakega prijavljenega naročnika v pomnilniku dovolj pripravljenih svežih parov RAND in SRES, ki jih vnaprej dobi od podsklopa AUC. Algoritem A3 naj bi bil izbran tako, da bi preprečil izračun ključa Ki iz zajetih parov RAND in SRES. Prav pri algoritmu A3 pa je bila prva šibka točka varnosti v sistemu GSM. Ko se je pričel uvajati sistem GSM, operaterji niso razumeli pomena vzorčnega algoritma A3 imenovanega COMP128 in so ga pričeli uvajati množično. To se je kasneje pokazalo za problematično. Pred tremi leti so namreč ameriški študentje odkrili, da vsebuje COMP128 pomankljivost, in da se da v določenem primeru, iz ne tako velikega števila parov RAND – SRES, izračunati vrednost Ki.

Zaupnost pogovora in prenašanih podatkov na radijski poti med mobilnim terminalom in bazno postajo je zagotovljena z šifriranjem. Za šifriranje se uporablja algoritem A5. Zaradi prilagajanja mednarodnim razmeram je v GSM sistemu v fazi 2 možnih 7 različic algoritma A5 in osma z odprtimi podatki. Šifrirajo se samo podatki na radijski poti med mobilnim terminalom in bazno postajo. Odprti podatki se v mobilnem terminalu in bazni postaji organizirajo v bloke, ki se oddajo v časovnih presledkih. Bloki se preko XOR vrat seštevajo s tokom ključev iz generatorja z algoritmom A5. Vrednosti ključev za šifriranje nadzoruje ključ Kc, ki je rezultat algoritma A8 na SIM kartici in v AUC med avtentikacijskim postopkom. Izračunan je iz istega RAND in Ki kot SRES s pomočjo algoritma A3. Ta način ima prednost, da ni potrebno zaradi šifriranja uvesti dodatnih vhodnih podatkov. Še več, če bi se slučajno proces avtentikacije obšel brez primerjave SRES v VLR, bi imela mobilni terminal in bazna postaja različne Kc za šifriranje podatkov in sporazumevanje bi bilo nemogoče. Dolžina ključa Kc je bila najprej 54 bitov, v zadnjem času pa se uporablja 64 bitna dolžina ključa. Kljub le 54 bitni dolžini pa še danes v svetu ni znanih primerov “Real time” prisluškovanja s prestrezanjem podatkov na radijski poti.

Rezultati SRES, z naključnim številom RAND in ključem za šifriranje Kc tvorijo tako imenovan “Triplet”. V sistemu GSM je šifriranje signala uporabljeno le na radijski poti. Povsod drugod v sistemu je signal nešifriran in tu je zaščita izvedena na enak način kot je to izvedeno v klasični telefoniji, z zaščito dostopa do komunikacijskih linij.

Postopek šifriranja se lahko prične šele po uspešnem prepoznavanju SIM kartice. Za zagon avtentikacijskega postopka mora SIM kartica preko radijske poti poslati svojo identiteto nešifrirano. Da bi onemogočili prepoznavanje naročnika s prisluškovanjem na radijski poti, dodeljuje sistem naročnikom začasne številke TMSI (Temporary Mobile Subscriber Identity). Številka IMSI (International Mobile Subscriber Identity) vezana na SIM kartico, torej na naročnika, se prenaša po radijski poti samo pri prvem vklopu telefona po sklenitvi naročniškega razmerja ali, če iz nekega razloga TMSI ni poznan omrežju. Od takrat naprej se zaradi principa varovanja naročnikove identitete uporablja le od omrežja dodeljena začasna številka TMSI, ki jo terminal vpiše tudi na kartico SIM. Pri identifikaciji se skupaj s TMSI uporablja še koda LAI (Location Area Identity). Preko LAI omrežje prepozna kje je bil uporabnik nazadnje prijavljen. Če se uporabnik prijavlja v novo omrežje, to dobi od prejšnjega omrežja IMSI uporabnika. Prenašanje številke IMSI preko fiksnih linij pa je dosti bolj varno, kot po radijski poti.

V praksi je za varnost potrebno poskrbeti še pri upravljanju s ključi Ki. Kot smo že prej videli, se ti nikoli ne prenašajo izven varnega okolja kartice SIM ali omrežnega podsklopa AUC. Toda pri prenašanju ključev od proizvajalca kartic SIM do AUCja je potrebno poskrbeti za odgovarjajočo varnost. Pri tem pomaga standardizirano šifriranje podatkov Ki, ki so izven prej omenjenih varnih okolij vedno šifrirani z algoritmom imenovanim A4.

Če primerjamo zahteve in varnostne funkcije vpeljane v omrežja GSM, se takoj pokažejo pomanjkljivosti.

- Prva in po splošnem mnenju največja luknja v varnosti je dejstvo, da telefon, oziroma kartica SIM, ne preverja, če je prijavljena v pravo

omrežje z enako zanesljivostjo, kot omrežje preverja identiteto kartice SIM.

- Druga pomanjkljivost je ta, da so govorni signal ali prenašani podatki šifrirani le na radijski poti, torej med telefonom in bazno postajo, drugod pa se pojavljajo v odprti obliki in so zaščiteni le s fizično zaščito dostopa.

- Tretja slabost v varnosti je dejstvo, da terminal nima načina, da bi preveril ali so sprejeti sistemski podatki pristni in ali res izvirajo od pravega podsklopa omrežja.

- Kot četrto slabost lahko štejemo, da je od zasnove sistema GSM do danes zaradi napredka računalniške tehnologije nivo zaščite upadel zaradi samega načina šifriranja ali zaradi premajhne bitne dolžine ključev.

GSM tehnologiji lahko iz vidika varnosti zamerimo še spodnje pomankljivosti.

- Domače omrežje nima nadzora nad načinom uporabe »tripletov« v drugih omrežjih roaming partnerjev. To pomeni, da je lahko en komplet podatkov uporabljen za nadzor dostopa do storitev za ves čas gostovanja naročnika. Domače omrežje takega ravnanja, ki je gotovo slabo v varnostnem pogledu, ne more preprečiti.

- Varnostne funkcije nimajo vgrajenih principov prilagodljivosti. V sistemu se, na primer, ne da spremeniti šifrirnega algoritma, če bi bilo to potrebno.

- Uporabnik nima nadzora nad tem, ali omrežje v katerem je prijavljen s šifriranjem zaščiti njegov pogovor ali prenešene podatke.

III. IZBOLJŠANA VARNOST V OMREŽJIH UMTS

Varnost v omrežjih 3G je osnovana na preskušeni varnosti omrežij 2G z dodatnimi varnostnimi ukrepi, ki odpravljajo prej opisane pomanjkljivosti v omrežjih GSM. Tako izbrana osnova varnosti ima poleg preskušene zanesljivosti še to prednost, da omogoča kompatibilnost navzdol. Torej uporabniku omogoča varen dostop do storitev omrežij UMTS in GSM **[2]**.

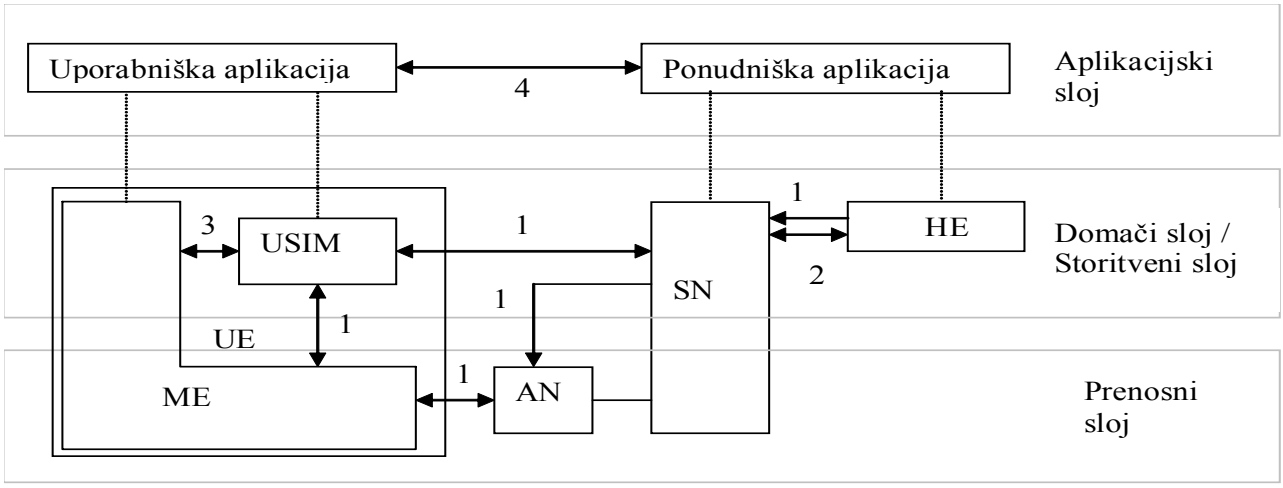
Varnost je zasnovana na spodnjih petih načelih:

1. Varnost dostopa do storitev omrežja.
2. Varnost prenašanih podatkov med sklopi znotraj omrežja ponudnika storitev.
3. Varnost dostopa do mobilnega terminala.
4. Varnost izmenjave podatkov med mobilnim terminalom in sklopi omrežja ponudnika storitev.
5. Načelo, da je uporabnik obveščen o tem, če je varnostna funkcija aktivna ali ne in ali je storitev do katere dostopa odvisna od varnostnih funkcij.

Zaradi mednarodno poenotenega UMTS sistema lahko uporabnik uporablja storitve omrežja tudi kot gost v drugih omrežjih. Storitve v drugih omrežjih so omejene le z zmožnostmi omrežja kjer uporabnik gostuje in s sporazumom med operaterjem domačega omrežja (HPLMN - Home Public Land Mobile Network) in operaterjem omrežja v katerem uporabnik gostuje (VPLMN-Visiting Public Land Mobile Network). Zato poskrbi večslojni proces upravljanja z omrežji, zaračunavanja prometa in storitev varovanja. Tako za avtentikacijo naročnika, prenos za to potrebnih podatkov in za zaračunavanje prometa skrbi domače omrežje, gostujoče omrežje pa poskrbi za dejansko prepoznavanje, za vključitev v omrežje in merjenje prometa.

Vse, kar je potrebno za vključitev naročnika v omrežje, je poleg aktivacije v AUC/HLR tako imenovana kartica USIM (User Services Identity Module), vstavljena v UMTS ME (Mobile Equipment). Dostop do storitev UMTS omrežij je mogoč tudi z SIM kartico, seveda z nižjim nivojem varnosti. V nadaljevanju bo privzeto, da je v ME vstavljena kartica USIM. Na njej so zapisani vsi potrebni naročniški podatki, kot je mednarodna naročniška številka IMSI (International Mobile Subscriber Identity) in vsi drugi podatki potrebni za avtentikacijo UMTS naročnika, omrežja in postopka za dogovor za ključe. V samem mobilnem terminalu ni nobenih podatkov o naročniku. V njem je le na varen način shranjena serijska številka IMEI (International Mobile Equipment Identity). Z vstavljanjem USIM v terminal, se ta deli na radijski del (ME) in na naročniški del (USIM), kar omogoči operaterju, ki je izdal USIM kartico, celovit nadzor nad naročenimi storitvami in podatki, ki se nanašajo na varnost. USIM kartica je torej del celovitega sistema varovanja UMTS omrežja in omogoča naročnikovo mobilnost.

Kot dodatek, ki ne vpliva na varnost omrežja, vpliva pa na varno uporabo storitev, je dodano še:



Slika 1: UMTS varnostni mehanizmi

Legenda k sliki 1:

- ME – Mobile Equipment, Mobilni terminal
- USIM - User Services Identity Module kot del UICC (Universal Integrated Circuit Card)
- UE – User Equipment, Uporabniški terminal (ME + USIM)
- HE – Home Enviroment, Domače okolje
- SN – Service Network, Storitveno omrežje
- AN - Access Network, Omrežje dostopanja

Na sliki 1 so prikazani štirje varnostni mehanizmi:

1. *Varovanje dostopa do omrežja:* To je nabor varnostnih funkcij, ki omogočajo uporabnikom varno dostopanje do UMTS storitev in v popolnosti ščitijo omrežje pred nepooblaščenimi vdori na radijski povezavi.

2. *Varovanje v omrežni domeni:* To je nabor varnostnih funkcij, ki omogočajo vozliščem v domeni ponudnika 3G storitev, da varno izmenjujejo signalizacijske podatke in ščitijo pred vdori na žičnih signalizacijskih linijah.

3. *Varovanje v uporabniški domeni:* Je nabor varnostnih funkcij, ki varujejo dostop do mobilnih terminalov.

4. *Varovanje aplikacijski domeni*: Nabor varnostnih funkcij, ki omogočajo, da se varno izmenjujejo podatki med uporabniško in ponudniško domeno.

5. *Stanje in nastavljivost varnosti:* To je nabor varnostnih funkcij, ki omogočajo uporabniku, da je obveščen o tem, če je varnostna funkcija pri postopku uporabljena in ali je varnostno funkcijo potrebno uporabiti pri uporabi določene storitve **[7]**.

1. Varovanje dostopa v omrežje

Ta skupina varnostnih lastnosti združuje funkcije za zagotavljanje varovanja identitete, avtentikacije uporabnika, zaupnosti podatkov na povezavi pri dostopu, pristnosti sistemskih podatkov na povezavi pri dostopu in kot dodatek prepoznavanje mobilnega terminala, kar pa ni varnostna lastnost.

a. Varovanje identitete

To je lastnost, da se pri prihodu uporabnika na neko področje njegove identitete ne more prestreči na radijski poti in tudi, da se njegove trenutne lokacije ne more odkriti s prestrezanjem podatkov pri njegovem dostopanju do različnih storitev omrežja.

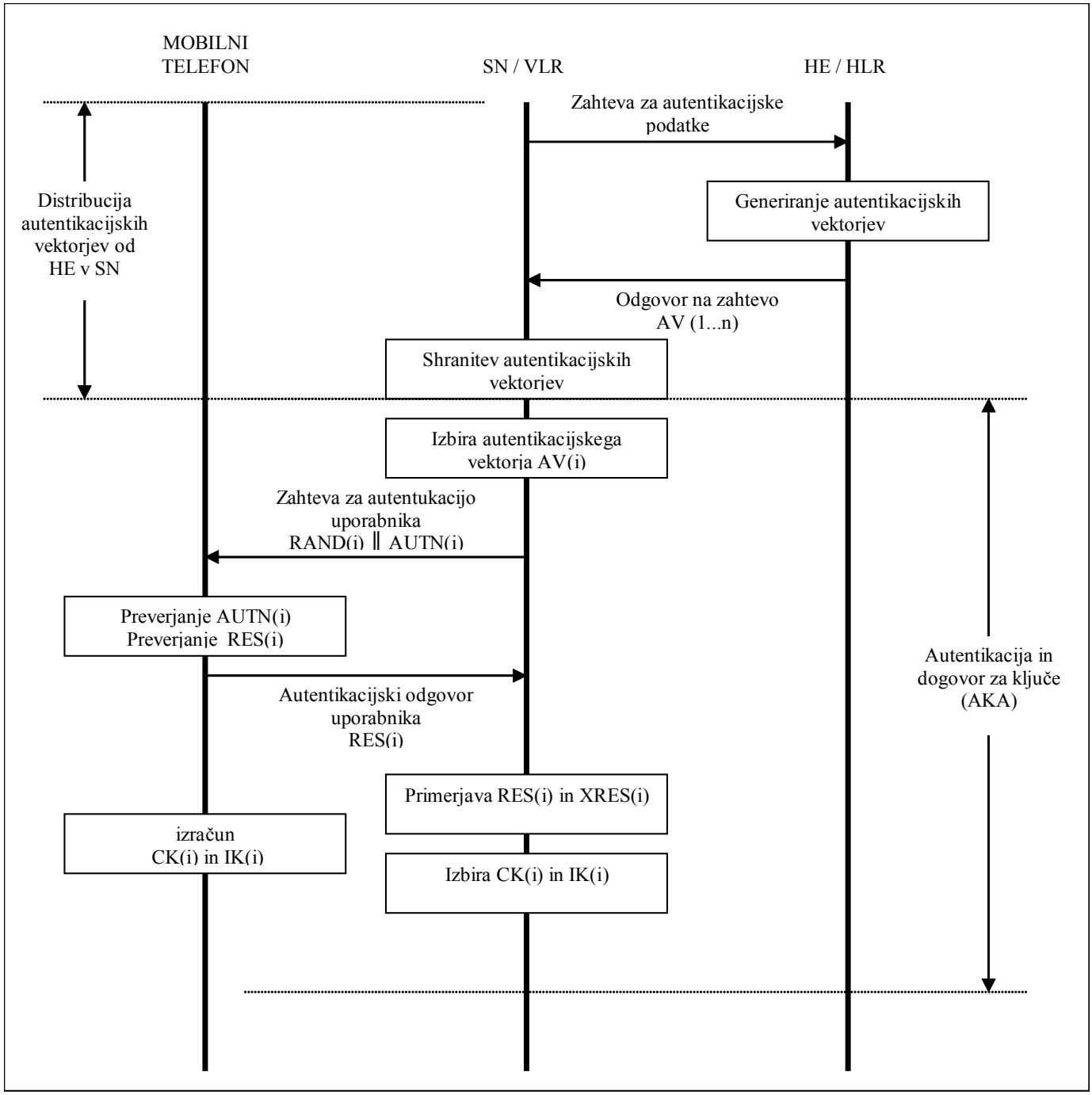
Ta lastnost je izvedena z uporabo začasne identitete, ki ima le lokalni značaj. Številka se imenuje TMSI – Temporary Mobile Subscriber Identity. Omrežje osvežuje TMSI je ob LU – Location update dogodkih. Za kasnejšo uporabo zapiše mobilni terminal TMSI na USIM. Oddajanje naročniku lastne številke IMSI – International Mobile Subscriber Identity preko radijske poti v nezaščiteni obliki je zelo omejeno. Le v redkih primerih, ko SN ne prepozna mobilnega telefona se v HE pošlje sporočilo z zahtevo za avtentikacijo v katerem je IMSI v odprti obliki. Tak primer je prvo

naročnikovo prijavljanje v omrežje po sklenitvi naročniškega razmerja.

b. Prepoznavanje identitete in dogovor za ključe

To je avtentikacijski postopek s pomočjo katerega ponudnikovo omrežje prepozna uporabnika, tako da ima ta pravico dostopa v omrežje, in v katerem ponudnikovo omrežje prepozna, da je pooblaščeno od uporabniške domene za nudenje storitev. V avtentikacijski postopek je vključen skriti ključ, ki je vpisan le v USIM uporabnika in v HE AUC. K temu je dodana lastnost, da USIM in HE vsak zase hranita SEQN zaporedno število avtentikacijskega postopka, ki je aktivno vključeno v avtentikacijo. Avtentikacija je s sistemom vprašanje – odgovor podobna GSM avtentikaciji, saj je na ta način zagotovljena najboljša skladnost obeh sistemov. Celoten pregled poteka avtentikacije prikazuje slika 2. V sliki 2 znak ‖ pomeni medsebojno spajanje.

Natančnejši opis sledi, zato naj se tu poudarijo bistvene novosti. Kot prvo je dodano sekvenčno število SQN, na sliki 2 označeno z izrazom (i), ki z nadzorom stanja števca v kartici USIM in v podsklopu HE AUC



Slika 2: Potek avtentikacije

omogoča detektiranje poskusov dostopa do storitev z lažno identiteto. Ob enem to preprečuje večkratno uporabo istega avtentikacijskega vektorja (kvinteta) v SN. Parameter AUTN omogoča mobilnemu telefonu avtentikacijo omrežja SN, kar ni vgrajeno v varnost omrežij GSM **[7]**.

Opis postopka avtentikacije in dogovora za ključe

Za izpolnitev zahtev iz prejšnjega odstavka je potrebnih šest kriptografskih funkcij in dve dodatni v primeru ponovne sinhronizacije sekvenčnega števila SQN:

f0 Funkcija za generiranje naključnega vprašanja RAND (Random chellenge)

f1 Algoritem za omrežno avtentikacijo za izračun MAC-A (Message avtentication code)

f1* Funkcija za resinhronizacijo pri postopku omrežne avtentikacije

f2 Funkcija za uporabnikovo avtentikacijo XRES (Expected user response)

f3 Funkcija za izračun šifrirnega ključa CK (Cipher key)

f4 Funkcija za izračun ključa za preverjanje pristnosti IK (Integrity key)

f5 Funkcija za izračun ključa za anonimnost AK (Anonymity key)

f5* Funkcija za izračun ključa za anonimnost AK v primeru resinhronizacije

- V okolju AUC se v sistemu GSM izračunajo tripleti. V sistemu UMTS se izračunajo kvinteti po sledečem postopku:

RAND = f0 n

MAC-A = f1k(SQN ‖ RAND ‖ AMF)

Parameter AMF (Authentication Management Field) je predviden za uporabo v HE. Operater lahko s pomočjo tega parametra vpliva na funkcijo f1. Recimo lahko priredi algoritem, uporabi drug algoritem ali izbere drug skrivni ključ K, če ima naročnik na kartici USIM na voljo več ključev in algoritmov.

XRES = f2k(RAND)

CK = f3k(RAND)

IK = f4k(RAND)

Če je zahtevano prikrivanje sekvenčnega števila SQN, se dodatno k zgornjim parametrom doda še ključ za anonimnost.

AK = f5k(RAND)

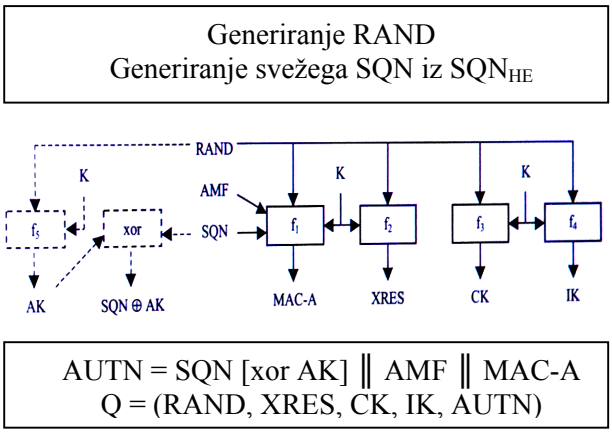
Sekvenčno število SQN se prikrije s tem, da se izvrši SQN xor AK. Prikrivanje SQN ni obvezno. Nazadnje HLR/AUC sestavi še avtentikacijski dokaz (token) AUTN.

AUTN = SQN [xor AK] ‖ AMF ‖ MAC-A

in kvintet Q je sestavljen:

Q = (RAND, XRES, CK, IK, AUTN).

Zgornji potek prikazuje slika 3.



Slika 3: AUC, Določitev parametrov avtentikacije

- V kartici USIM poteka podoben postopek. Ko VLR ali SN izbere kvintet, pošlje preko radijske poti RAND in AUTN. Po sprejemu zahteve, to je sprejemu para AUTN in RAND, USIM preveri, če je AUTN sprejemljiv. Če je, izračuna RES in ga pošlje v VLR ali SN. Ob tem izračuna še šifrirni ključ CK in ključ za zagotavljanje pristnosti podatkov IK. VLR ali SN primerja RES in XRES. Če se ujemata, izbere iz kvinteta CK in IK. V USIM in v HLR ali SN se CK in IK posredujeta sklopom, ki bodo skrbeli za zaupnost in pristnost podatkov. Sklopi so na USIM strani v

mobilnem telefonu in na VLR / SN strani v sklopu RNC.

Postopki v USIM potekajo na sledeč način:

Če je zahtevano prikrivanje SQN, se izračuna

AK = f5k(RAND).

Za tem se regenerira iz AUTN sekvenčno število

SQN = (SQN xor AK) xor AK

USIM izračuna

XMAC–A = f1k(SQN ‖ RAND ‖ AMF)

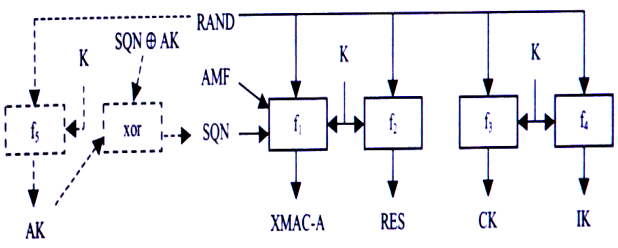
in primerja XMAC-A z MAC-A sprejetim v AUTN. Če sta različna, telefon pošlje v nazaj v VLR / SN odgovor z oznako, da je prišlo do napake pri preverjanju izvirnosti in prekine postopek. Če se XMAC-A in MAC-A ujemata, se postopek nadaljuje s preverjanjem, če se sprejeto sekvenčno število SQN ujema z lastnim SQN. Pri nadzoru nad SQN je predvideno nekaj svobode, tako da lahko operater to prireja svojim potrebam. Vendar pa morajo biti upoštevane mere za nadzor nad prelivanjem števcev in nekaj svobode pri nezaporedni uporabi kvintetov.

Če SQN ni sprejemljiv, USIM izračuna resinhronizacijski dokaz (token) AUTS in mobilni telefon odda uporabnikov avtentikacijski odgovor nazaj v VLR / SGSN skupaj z oznako, da je prišlo do sinhronizacijske napake in prekine postopek.

Če se sekvenčni števili SQN ujemata, USIM izračuna odgovor RES = f2k(RAND) in ga preko ME pošlje nazaj v VLR ali SGSN z oznako, da je uspešno sprejel avtentikacijsko zahtevo.

Končno se v USIM izračuna še šifrirni ključ CK = f3k(RAND) in ključ za preverjanje pristnosti IK = f4k(RAND).

Postopki so prikazani na sliki 4.



Slika 4: USIM, Določitev parametrov avtentikacije

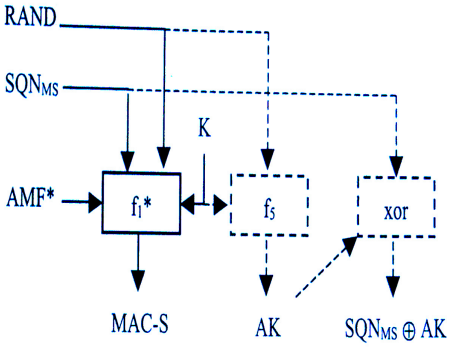
- V kartici USIM se resinhronizacijski postopek začne z izračunom

MAC–S = f1*k(SQNMS ‖ RAND ‖ AMF*).

AMF* je privzeta vrednost za AMF pri postopku resinhronizacije in je iz samih ničel. Če je zahtevana zaščita SQNMS se izračuna ključ AK = f5*k(RAND) in zatem SQNMS xor AK. Tako se lahko sestavi resinhronizacijski odgovor, ki je

$$AUTS = SQN_{MS} [xor\ AK] \| MAC\text{-}S.$$

Postopek je prikazan na sliki 5.



$$AUTS = SQN_{MS} [xor\ AK] \| MAC\text{-}S.$$

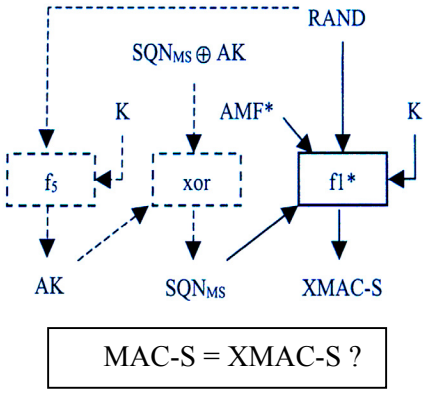
Slika 5: USIM, Resinhronizacija

- Po sprejemu podatka o sinhronizacijski napaki in para (AUTS, RAND) steče v HLR/AUC podsklopu postopek sinhronizacije.

Če je zahtevana zaščita SQNMS, HLR/AUC izračuna ključ AK = f5*k(RAND) in odkrije prikrito vrednost SQNMS = (SQNMS xor AK) xor AK. Če je SQNHE sprejemljiv za USIM, to pomeni naslednji SQN, se nadaljuje postopek s pošiljanjem avtentikacijskega vektorja s tem sekvenčnim številom. Če pa izračunan SQNHE ni sprejemljiv, potem HLR/AUC izračuna

XMAC–S = f1*k(SQNMS ‖ RAND ‖ AMF*),

kjer je AMF* privzeta vrednost za primer resinhronizacije.



Slika 6: AUC, Resinhronizacija

Če se MAC-S in XMAC-S ujemata, HLR/AUC postavi števec SQNHE na vrednost SQNMS. HLR/AUCE pošlje nove avtentikacijske vektorje in postopek avtentikacije se ponovi.

c. Zaupnost podatkov na povezavi pri dostopu

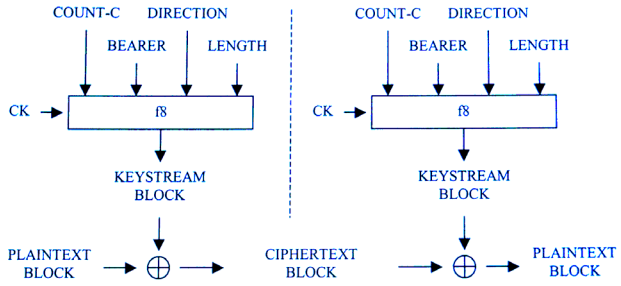
Zaupnost je zagotovljena z uporabo šifriranja z ustreznim algoritmom. Šifrirajo se prenašani podatki med mobilnim telefonom MS in omrežjem SN. Za razliko od sistema GSM, kjer so se šifrirali podatki le med mobilnim telefonom in bazno postajo, so tu šifrirani na celotni poti med mobilnim telefonom in sklopom za nadzor radijskega omrežja RNC. Postopek določitve skrivnega šifrirnega ključa CK je del avtentikacijskega postopka.

Sledeča slika 7 ponazarja uporabo funkcije f8 pri šifriranju odprtih podatkov z uporabo xor funkcije s tokom ključev. Regeneracija v odprte podatke je izvedena z uporabo podobnega postopka, to je uporaba xor funkcije na šifriranem signalu s tokom istih ključev kot so bili uporabljeni pri šifriranju.

Vhodni parametri so šifrirni ključ (CK), časovno odvisni vhod (COUNT-C), koda prenosa (BEARER), smer prenosa (DIRECTION) in zahtevana dolžina toka ključev (LENGTH). Na osnovi teh vhodnih parametrov algoritem f8 generira tok ključev (KEYSTREAM), ki šifrirajo bloke informacije odprtih podatkov (PLAINTEXT) v bloke šifriranih podatkov (CIPHERTEXT). Vhodni parameter LENGTH vpliva le na dolžino bloka KEYSTREAM BLOCK ne pa na vsebino bloka.

Za uporabo v UMTS omrežjih je bil za funkcijo f8 izbran algoritem osnovan na osnovi "Kasumi" algoritma. Funkcija f8 je vgrajena v mobilni telefon in v podsistem RNC.

- Znak $\oplus$ pomeni operacijo XOR



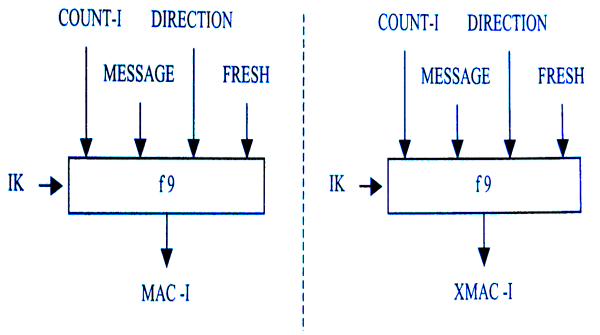
Slika 7: Postopek šifriranja

d. Pristnost sistemskih podatkov na povezavi pri dostopu

To je varnostna lastnost, ki preprečuje, da bi se sistemski podatki lahko neautorizirano spreminjali. Z drugimi besedami, ta varnostna funkcija preprečuje mobilnemu telefonu povezavo z lažno bazno postajo. To je novost v primerjavi z starejšimi generacijami mobilnih omrežij. Sistemski podatki v povezavi med mobilnim telefonom in dostopanim omrežjem so občutljivi in morajo biti celovito zaščiteni. UMTS algoritem za pristnost in ključ (IK) zagotavljata nadzor nad pristnostjo sistemskih podatkov. Ključ IK se določi med postopkom avtentikacije v delu AKA, kakor je bilo prikazano prej. Dejanski algoritem, ki bo uporabljen pri dostopu mobilnega telefona v omrežje SN, je rezultat njunega dogovora. Za omrežja 3G verzije 99 je bil izbrana funkcija f9 na osnovi algoritma "Kasumi". Na ta način lahko tako mobilni telefon kot omrežje SN preverjata pristnost sistemskih podatkov prihajajočih od telefona ali od omrežja.

Vhodni parametri v algoritem f9 so ključ IK, časovno odvisni vhodni parameter (COUNT-I), naključna vrednost generirana na strani omrežja (FRESH), bit za oznako smeri (DIRECTION) in signalizacijski podatek (MESSAGE). Na osnovi teh vhodnih podatkov uporabnik izračuna s pomočjo algoritma f9 avtentikacijsko kodo za pristnost sporočila (MAC-I), ki je pripeta sporočilu med pošiljanjem po radijski poti. Sprejemnik izračuna XMAC-I iz sprejetega sporočila na enak način kot je to storil pošiljatelj. Če sta MAC-I in XMAC-I enaka, je pristnost podatkov potrjena.

Potek je prikazan na sliki 8 **[3]**, **[6]**.



Slika 8: Postopek preverjanja pristnosti sistemskih podatkov

2. *Varovanje v omrežni domeni:*

V omrežju 3G verzije 99 ta skupina varnostnih funkcij še ni uporabljena. Kaj bo novega v naslednji verziji 00, je navedeno v zadnjem poglavju tega prispevka **[7]**.

3. *Varovanje v uporabniški domeni:*

Po definiciji je to avtentikacija uporabnika proti kartici USIM in avtentikacija kartice USIM proti mobilnemu telefonu.

Kartica prepozna pravega uporabnika ali skupino uporabnikov s pomočjo prikrite kode PIN, ki je varno spravljena v okolju kartice USIM. Uporabnik dobi pravico do dostopa do kartice USIM le po pravilnem vnosu kode PIN. Da nepooblaščeni ne bi uspel odkriti prikrite kode PIN, je uporabljen princip omejevanja števila ponavljanj vnašanja napačne kode. Ko je meja presežena, se kartica USIM zablokira. Ponovna aktivacija je mogoča s pravilnim vnosom kode za odklepanje PUK. Tudi vnosi kode PUK so nadzirani. Po preseženem največjem dovoljenem številu napačnih vnosov kode PUK se kartica za vedno zablokira.

Avtentikacija kartice USIM proti telefonu je namenjena za posebne namene, če se želi doseči, da se telefon lahko vključuje v omrežja le s kartico USIM določenega ponudnika storitev ali celo le z določeno kartico USIM **[1]**, **[7]**.

4. *Varovanje v aplikacijski domeni:*

UATK (USIM Application Tool Kit) omogoča ponudnikom storitev, da izdelajo aplikacije na kartici USIM. Če je potrebno varovanje preko omrežij prenašanih sporočil, se to vgradi z varnostnim nivojem, ki ga izbere ponudnik storitve.

Varnostne lastnosti UATK morajo omogočati:

- Avtentikacijo omrežja proti kartici USIM in kartice USIM proti omrežju,
- Pristnost sporočila,
- Zaznavanje ponavljanj,
- Potrjevanje sprejema in
- Zaupnost prenašanih podatkov

Sporočilo aplikacije se prenese iz pošiljajoče na sprejemajočo aplikacijo v enem ali več zavarovanih paketih (slika 9). Prenos informacije poteka preko oddajnega sklopa do enega ali do skupine sprejemnih sklopov. V tej verigi je sprejemni sklop odgovoren za rekonstrukcijo sprejetih zavarovanih paketov v obliko, ki je razumljiva za ciljno sprejemajočo aplikacijo. Kot je bilo omenjeno, lahko nastopa več sprejemnih sklopov in aplikacij.

Pred prenosom informacije mora oddajajoča aplikacija oddajnemu sklopu sporočiti varnostni mehanizem, ki bo uporabljen pri zaščiti sporočila **[4], [5], [7]**.

5. *Stanje in nastavljivost varnosti:*

Čeprav morajo biti v splošnem varnostne funkcije neopazne za uporabnika, je v nekaterih primerih, v skladu s skrbjo za naročnika, potrebno poskrbeti večjo preglednost delovanja varnostnih funkcij. To vodi v številne funkcije, ki obveščajo uporabnika o varnostno naravnanih dogodkih, kot so:

- Obveščanje o šifriranju pri dostopu do omrežja: To je lastnost, da je uporabnik obveščen, če je zaupnost prenašanih podatkov po radijski poti zagotovljena. Še posebno je to pomembno v primeru, ko uporabnik vzpostavi nezaščiteno povezavo.

- Obveščanje o nivoju zaščite: To je lastnost, da je uporabnik obveščen o nivoju zaščite, ki jo nudi omrežje v katerem gostuje, še posebno takrat, ko je premeščen ali gostuje v omrežju z nižjim nivojem varnosti. Tak primer je premestitev iz omrežja 3G v omrežje 2G.

Sledeča lastnost, ki mora biti zagotovljena, je lastnost, da lahko uporabnik izbrano storitev uporabi ali ukrepa v odvisnosti od nivoja varnosti aktivirane varnostne funkcije. Storitev se lahko uporabi le v primeru, ko so aktivne vse varnostne funkcije, ki se nanašajo na to storitev in jih je nastavil uporabnik. Priporočene so sledeče lastnosti za nastavljivost:

- Vklop in izklop avtentikacije uporabnika proti kartici USIM: Uporabnik mora imeti možnost nadzora nad avtentikacijo uporabnika proti

kartici USIM. Na primer pri nekaterih dogodkih, storitvah ali uporabi.

- Odgovor na ali zavrnitev nezaščitenih dohodnih klicev: Uporabnik mora imeti možnost, da zavrne klic, katerega komunikacija ni šifrirana.

- Klicanje ali ne v primeru nezaščitene komunikacije: Uporabnik mora imeti možnost, da kliče ali pa ne v omrežju, ki nima omogočenega šifriranja prenašanih podatkov.

- Privzem ali zavrnitev določenih šifrirnih algoritmov: Uporabnik mora imeti možnost nadzora in izbire, kateri šifrirni algoritem je sprejemljiv za uporabo **[7]**.

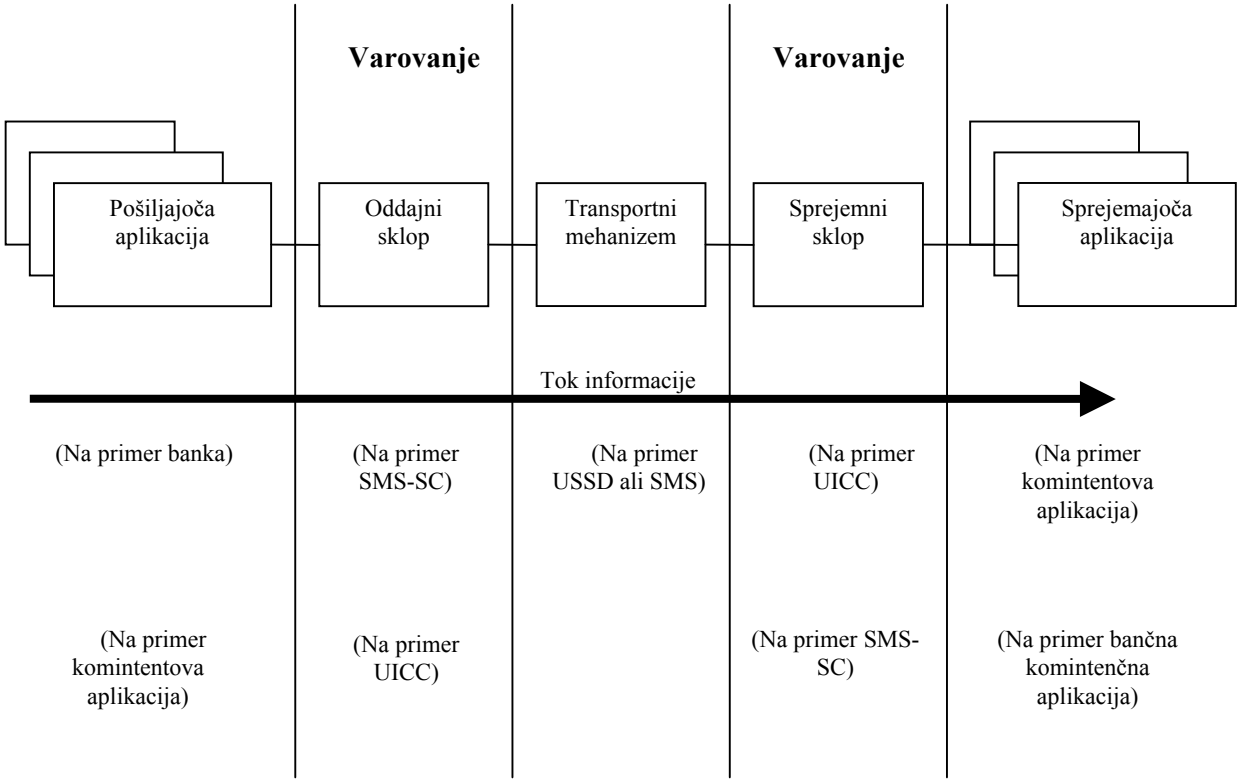
IV. VARNOST PRI PRENOSU KLJUČEV

V splošnem je varnost celotnega sistema enaka varnosti najšibkejšega člena v verigi varnostnih ukrepov. V prejšnjem opisu ni zajetega še enega zelo pomembnega varnostnega področja, to je varovanje prenosa ključev iz okolja proizvajalca kartic USIM v okolje podsistema HLR/AUC. Ta segment varnosti večinoma ni zajet sistemsko. Prenos podatkov se ponavadi izvede s pomočjo šifriranja z algoritmi, ki so vgrajeni v podsistem HLR/AUC. V ta namen je v sistemih GSM in UMTS namenjen algoritem A4. Tako se ključ K nikoli ne pojavi v odprti obliki in je znan le proizvajalcu kartic USIM.

Enako je s ključi, ki so temelj varnosti v aplikacijski domeni.

V. ZAKLJUČEK ALI KAJ SE ŠE PRIČAKUJE NA PODROČJU VARNOSTI?

Prispevek je pokazal, da je omrežje UMTS zadržalo v veliki meri kompatibilnost z omrežjem GSM. Lastnosti, ki so se izkazale v omrežju GSM kot odporne in zanesljive, so se v omrežju 3G obdržale v izboljšani obliki. Izboljšave so odpravile opažene, dejanske ali pa le zaslutene pomanjkljivosti. Te lastnosti so sedaj vgrajene v omrežju UMTS verzije 99.



Slika 9: UATK, Potek postopka

V načrtih za verzijo 00 so v postopku še dodatne izboljšave.

Varovanje v omrežni domeni: Za verzijo 00 je predvideno, da bodo sklopi omrežja, predvsem tisti sklopi, ki pripadajo različnim operaterjem, imeli možnost, da pred izmenjavo podatkov drug drugega prepoznajo. V igri sta načina: MAP zaščita na nivoju aplikacij, ki naj predpiše zaščito MAP signalizacije in način za uporabo pri signalizaciji znotraj in med hrbteničnimi omrežji, kot je MAP, CAP, GTP. Ti

mehanizmi bodo potrebovali mehanizem za distribucijo ključev, ki bo standardiziral podporo medsebojne povezave operaterjev in znotraj hrbteničnih omrežij, ki jih upravlja več ponudnikov.

IP multimedijske storitve: Te storitve vključujejo različne aplikacije kot so zvok, video in podatki. Definirati bo potrebno postopke za zagotavljanje medsebojnega zaupanja in varovanja pri komunikaciji od uporabnika do ponudnika, v IP multimedijskem hrbteničnem omrežju ter v domeni paketnega ali komutiranega načina prenosa.

Izboljšave v programski opremi mobilnih telefonov: Tisti del programske opreme mobilnih telefonov, ki skrbi za izvajanje storitev s pomočjo naloženih programov, bazira na osnovi prepoznavanja zunanjih standardov. Ti standardi prihajajo v UMTS tako, da jih sedaj 3GPP vnaša kot reference v dokumente (recimo WAP). Iz vidika operaterja je najbolj pomembno, da tak razvoj upošteva varnostne funkcije na način, da se ohrani celovitost omrežja in se pri tem zagotavlja zaupnost in pristnost podatkov in aplikacije od uporabnika ali od ponudnika.

Uporaba šifriranja po celem omrežju: V verziji 00 bodo morda že izdelane nove zahteve ali pa se bodo že pokazale priložnosti, da se vnese v omrežje razširjeno zaščito za zagotavljanje zaupnosti podatkov po celem hrbteničnem omrežju. To bi omogočilo zaščito celotne komunikacijske poti od uporabnika do uporabnika. Pri tem je potrebno upoštevati, da se kljub zaščiteni komunikaciji omogoči legalno prestrezanje podatkov.

FIGS (Fraud Information Gathering System) izboljšave: Ta sistem je bil zasnovan že v sistemu GSM, pa ni nikoli prav zaživel. Namen tega sistema je detektiranje primerov obnašanja naročnikov s povečanim sumom na zlorabe storitev mobilnega omrežja med roamingom. Ta funkcionalnost se mora razširiti na storitve s paketnim načinom prenosa.

Razmišlja se še o varovanju dostopa do storitev preko zasnove imenovane OSA (Open Service Architecture). To omogoča operaterju in zunanjemu ponudniku uporabo funkcionalnosti omrežja preko OSA vmesnika. Aplikacije so lahko nameščene izven hrbteničnega omrežja, na razpolago pa so preko OSA vmesnika. Aplikacije lahko pripadajo domeni omrežja operaterja, čeprav tečejo izven hrbteničnega omrežja. Tako kot prej je iz vidika operaterja je najbolj pomembno, da tak razvoj upošteva varnostne funkcije na način, da se ohrani celovitost omrežja in se pri tem zagotavlja zaupnost in pristnost podatkov in aplikacije od uporabnika ali od ponudnika.

LITERATURA

[1] 3GPP, TS 22.022 v3.0.1
[2] 3GPP, TR 31.900 v5.1.0
[3] 3GPP, TS 35.206 v4.0.0
[4] ETSI, TS 122 048 v4.0.0
[5] ETSI, TS 123 048 v5.5.0
[6] ETSI, TS 133 105 v4.1.0
[7] ETSI, TS 133 102 v5.1.0

Leopold Šolc je zaposlen v družbi Mobitel kot vodja službe za preprečevanje zlorab storitev v mobilnih omrežjih. Sodeluje pri načrtovanju, implementaciji in vzdrževanju vseh delov mobilnih omrežij NMT, GSM in UMTS, ki vplivajo na varnost storitev in naročnika. Od leta 1998 je član GSMA Fraud Foruma.